**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:
Marc Epstein et al.

Application No.: 09/750,500

Filed: December 28, 2000

For: Architecture For Serving And Managing Independent Access Devices

Confirmation No.: 6952

Group Art Unit: 2157

Examiner: El Chanti, Hussein A.

Attorney Docket No.: 300-2

**VIA EFS**
Mail Stop Appeal Brief - Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

## APPEAL BRIEF

SIR:

This is Appellant's brief under 37 C.F.R. § 41.31 for the appeal of the Final Office Action mailed September 23, 2008, by Examiner Hussein A. El Chanti, in the above-referenced patent application.

**REAL PARTY IN INTEREST**

The real party in interest is CenterBeam Inc., the assignee of record.

**RELATED APPEALS AND INTERFERENCES**

There are no other appeals or interferences which bear on the present appeal.

**STATUS OF CLAIMS**

Claims 1-39, 45-46, 56-57, and 63 are canceled and claims 40-44, 47-55, 58-62, and 64-67 are rejected. Applicants appeal the rejection of claims 40-44, 47-55, 58-62, and 64-67.

**STATUS OF AMENDMENTS**

Claims 45, 56, and 63 have been canceled with the filing of this Appeal Brief in accordance with the provisions of Rule 37 C.F.R. § 41.33.

**SUMMARY OF CLAIMED SUBJECT MATTER:**

Herein, a brief introduction is provided to the general concepts covered by the independent claims, with reference to the application, to provide some context for, and to render more concise the subsequent description of the individual independent claims.

Aspects of the invention claimed herein are directed to a service provider that provides services to client computers, in which a first set of services is provided by a first set of servers having a first one-way trust relationship with the client computers and a second set of servers having a second one-way trust relationship, opposite the direction of the first one-way trust relationship, with the client computers.

The concept of a one-way trust is now expanded upon with reference to the specification. The specification recites that "a trust . . . allows users in one of the sets of computers to access resources in another set of computers in a secure way". Specification, page 5, lines 24-25. Attention is now directed to page 7 and Figure 2 of the specification. Figure 2 includes illustrations of links 221-226 and 231-236 wherein the arrows on the links indicate which forests trust other forests. See Specification, page 7, lines 14-15. Moreover, the Specification indicates that there are no two-way trusts in the depicted arrangement. See Specification page 7, line 18.

For example, directing attention to link 232 and the arrow thereon, the specification states that forest 207 trusts forest 204 (with the arrow directed toward forest 204), but that forest 204 does *not* trust forest 202, which is consistent with the arrow on the link between forests 202 and 204 being directed away from forest 202 (see specification, page 7, lines 19-20). Thus, the links of Figure 2 show one-way trusts with the direction of trust indicated by the arrows on the respective links. Hereafter, Mgt./Conf. Forest 204 is referred to as management forest 204.

It is the trusted entity which is granted secure access to the trusting entity. For example, with reference to Figure 2 and to page 8, lines 9-11, client 208 allows management forest 204 to access client 208 to provide a software update thereto, which is consistent with link 233 having a one-directional trust direction from client 208 to management forest 204. Thus, secure access is provided in the direction opposite the direction of the trust direction shown by the arrowed links in Figure 2.

The subject matter can be analogized to the following system, in which the secure access is implemented with the typical methodology of requiring a user name and password so the user can be authenticated. Consider a terminal connected to a first host computer, wherein the terminal has to provide a user name and login password in order to access the first host computer. The first host computer provides some services to the terminal. Now consider that there are other services provided to the terminal by a different, second, host computer. For these other services, the terminal does not log into the second host computer and provide a user name and login password. Instead, the second host computer logs into the terminal, and provides to the terminal the user name and login of the second host computer. The terminal then receives services from both hosts.

For purposes of explanation herein, the user terminal logs onto the first host in a secure manner to receive services, but the user terminal is logged onto by the second host to receive other services. Therefore, each host is connected to the user terminal using back to back secure access connections, namely, the connections are secure in opposite directions to one another.

Claim 40 recites:

> providing a first set of services on a first set of one or more servers of the service provider to the plurality of client computers by providing secure access to the first set of one or more servers by the plurality of client computers,
>
> but prohibiting secure access to the plurality of client computers by the first set of one or more servers,

In the aspect of the invention of claim 40, with reference to Figure 2, server forest 202 is the first set of one or more servers, and one or more of entities 206-211 are the client computers. Arrowed links 221-226 identify a one-way trust relationship in which server forest 202 trusts the plurality of client computers. Correspondingly, as discussed above, the plurality of client computers is provided secure access to the first set of one or more servers.

Consistent with the above discussion, the one-way character of the trust indicated by arrowed links 221-226 operates to *prohibit* secure access to the plurality of client computers 206-211 by the first set of one or more servers 202. This is consistent with management forest 204 not trusting service forest 202, as discussed in the specification at page 7, lines 19-20, discussed above.

Claim 40 further recites:

> providing a second set of services on a second set of one or more servers of the service provider to the plurality of client computers by providing secure access to the plurality of client computers by the second set of one or more servers,
>
> but prohibiting secure access to the second set of one or more servers by the plurality of client computers.

In the aspect of the invention recited in claim 40, the second set of servers is management forest 204 (see Figure 2). In a parallel manner to the discussion of the earlier portion of claim 40 above, with reference to Figure 2, arrowed links 231-236 establish a one-way trust extending from client computers 206-211 to management forest 204. Consistent with the introductory discussion above, this one-way trust corresponds to providing secure access to the plurality of client computers 206-211 by the second set of one or more servers 204, but prohibiting secure access to the second set of one or more servers 204 by the plurality of client computers 206-211.

Claim 51 is directed to a system and closely tracks the language of method claim 40. Claim 51 recites:

> a first set of one or more servers for providing a first set of services to the plurality of client computers by providing secure access to the first set of one or more servers by the plurality of client computers,
>
> but prohibiting secure access to the plurality of client computers by the first set of one or more servers;

With reference to Figure 2, arrowed links 221-226 extend from first of servers 202 to client computers 206-211, respectively, indicating the existence of one-way trusts between the listed entities. Thus, in accordance with the above discussion of trusts and the associated directions in which secure access is allowed (see Applicants' specification page 5, lines 23-25), the client computers 206-211 are provided secure access to the first set of one or more servers, but the first set of one or more servers are prohibited from securely accessing the plurality of client computers.

Claim 51 further recites:

> a second set of one or more servers for providing a second set of services to the plurality of client computers by providing secure access to the plurality of client computers by the second set of one or more servers,
>
> but prohibiting secure access to the second set of one or more servers by the plurality of client computers

Consistent with the above discussion, and with continuing reference to Figure 2, arrowed links 231-236 show the existence of one-way trusts extending from client computers 206-211, respectively, to management forest 204 (the second set of one or more servers). Thus, the second set of one or more servers 204 is provided with secure access to the plurality of client computers 206-211, but client computers 206-211 are prohibited from securely accessing the second set of one or more servers.

Claim 62 recites:

> "separating the services provided by the service provider into a first group of services provided by a first group of one or more servers of the service provider, and a second group of services provided by a second group of one or more servers of the service provider;"

The separation of services of claim 62 is discussed (a) between page 5 line 26 and page 6, line 3; and (b) on page 8, lines 3-8 and is best understood in relation to Figure 2 where the first group of one or more servers corresponds to server forest 202 and the second group of one or more servers corresponds to management forest 204.

Claim 62 further recites:

> "providing the first set of services from the first set of servers through a one-way trust connection from the first set of servers to the client computers"

In the aspect of the invention recited in claim 62, the one-way trust connection is shown by any of arrowed links 221-226 extending from server forest 202 to client computers 206-211.

Claim 62 further recites:

> "providing the second set of services from the second set of servers to the client computers through a one-way trust connection from the client computers to the second set of servers"

A one-way trust connection is shown by any one of arrowed links 231-236 extending from client computers 206-211 to management forest 204 (the second set of servers).

Since the subject matter of claim 66 and 67 is similar, the language of these claims is quoted below, and their features are discussed together thereafter.

Claim 66 recites:

> enabling a first set of services on a first set of servers of the service provider through a one-way trust connection from the first set of servers to the plurality of client computers;

enabling a second set of services on a second set of servers of the service provider to the plurality of client computers through a one-way trust connection from the client computers to the second set of servers; and

providing the first and second sets of services.

Claim 67 recites:

a first set of servers for providing a first set of services to the plurality of client computers through a one-way trust relationship from the first set of servers to the plurality of client computers; and
a second set of servers for providing a second set of services to the plurality of client computers through a one-way trust relationship from the plurality of client computers to the second set of servers.

The first and second sets of services are described on page 8, lines 3-8. The one-way trust connection from the first set of servers 202 to client computers has been discussed above, and is shown with arrowed links 221-226 of Figure 2. The one-way trust connection from the client computers 206-211 to the second set of servers 204 is shown with arrowed links 231-236 of Figure 2.

**Grounds of Rejection to be Reviewed On Appeal:**

A first issue presented for review is whether claims 40-44, 47-55, and 58-61 are unpatentable over U.S. Patent Number 6,557,169 to Erpeldinger (hereafter, "Erpeldinger") under 35 U.S.C. § 102 (e).

A second issue presented for review is whether claims 62, 64, and 65 are unpatentable over U.S. Patent Number 6,557,169 to Erpeldinger under 35 U.S.C. § 102 (e).

A third issue presented for review is whether claim 66 is unpatentable over U.S. Patent Number 6,557,169 to Erpeldinger under 35 U.S.C. § 102 (e).

A fourth issue presented for review is whether claim 67 is unpatentable over U.S. Patent Number 6,557,169 to Erpeldinger under 35 U.S.C. § 102 (e).

**Argument:**

**A. The rejection of Claims 40-44, 47-55, and 58-61 as Being Anticipated by Erpeldinger is Improper:**

In this section, independent claims 40 and 51 are discussed together.

Attention is directed first to the first paragraphs (paragraph (1)) of claims 40 and 51. The Examiner purports to supply the limitations of paragraph (1) above from col. 1, lines 22-32 of Erpeldinger (see OA, page 2, numbered section 2, lines 8-9). On page 5 of the Office Action, the Examiner reiterates this contention, asserting that the email and printing services discussed at col. 1, lines 22-32 of Erpeldinger meet the limitations of claims 40 and 51. The Applicants respectfully disagree.

The cited section of Erpeldinger provides a general introduction to the section labeled the "DESCRIPTION OF THE RELATE[D] ART" of Erpeldinger. The most pertinent section Applicants can identify in the cited passage recites that "a user may connect to several servers to use different services." Col. 1, lines 31-32. However, the cited passage, like the rest of Erpeldinger, is completely silent with respect to "providing secure access to the first set of one or more servers by the plurality of client computers" and "prohibiting secure access to the plurality of client computers by the first set of one or more servers" which are recited in paragraph (1) of claims 40 and of claim 51. Accordingly, the above-quoted limitations of paragraph (1) of claims 40 and 51 are not disclosed in Erpeldinger.

The Office Action cites to the passage between col. 2, line 65 and col. 3, line 22 of Erpeldinger as disclosing the limitations of paragraph (2) of claims 40 and 51. Erpeldinger describes a server 24 that is coupled to a plurality of workstations and that is operable to transfer application software, including a new operating system to one of the workstations, such as workstation 12, in the pertinent network. See col. 2 lines 59-65. This passage and the succeeding passage between col. 2, lines 65 and col. 3, line 22, suggest that server 24 is able to securely access workstation 12. However, nowhere do these passages disclose "prohibiting secure access to the . . .second set of one or more servers by the client computers" which is recited in paragraph (2) of claims 40 and 51.

In the response to arguments section on page 5 of the Final Office Action mailed 9/23/08, the Examiner contends that the software distribution function of Erpeldinger qualifies as "software distribution software" (see OA, page 5, lines 7-8). However, the remarks in this section are completely silent with respect to the feature of "prohibiting secure access to the second set of one or more servers by the plurality of client computers" as recited in claims 40 and 51. Moreover, no other portion of Erpeldinger discloses the pertinent features. Accordingly, Erpeldinger does not disclose the limitations of paragraph (2) of claims 40 and 51, as alleged in the Office Action. Based on the foregoing, Erpeldinger does not disclose all the limitations of claim 40 or 51. Accordingly, claims 40-44, 47-55, and 58-61 are patentable over Erpeldinger.

In short, Erpeldinger describes nothing more than – at best from the Examiner's viewpoint – a client computer that receives services from multiple servers. Applicant is not claiming to be the first to connect a client computer to multiple servers. As clearly recited in applicants' claims at issue, and as explained at least at pp. 5-7, in the present invention "there are no two way trusts" and back to back one way trusts are used between a client and each of two different sets of servers. Erperldinger's use of a client connected to two servers conventionally does not anticipate these claims.

**B. <u>The rejection of Claims 62, 64, and 65 As Being Anticipated by Erpeldinger is Improper:</u>**

On page 4 (fourth paragraph) of the Office Action mailed 9/23/08, the Examiner rejects all of claims 62-67 for "similar reasons" as claims 40-44, 47-55, and 58-61 without further elaboration. There are thus no detailed Office Action rejection remarks to respond to. Accordingly, the discussion below compares the features recited in independent claims 62, 66, and 67 to the teachings of Erpeldinger without making further reference to the Office Action remarks. To avoid repetition, some subject matter from Erpeldinger discussed in connection with claim 62 is referred back to in the discussions of claims 66 and 67 since many of the same claim terms are recited in these three independent claims.

Claim 62 is directed to a method to provide services to a plurality of client computers and recites:

> separating the services provided by the service provider into a first group of services provided by a first group of one or more servers of the service provider, and a second group of services provided by a second group of one or more servers of the service provider;
>
> providing the first set of services from the first set of servers through a one-way trust connection from the first set of servers to the client computers; and
>
> providing the second set of services from the second set of servers to the client computers through a one-way trust connection from the client computers to the second set of servers.

Applicants respectfully contend that Erpeldinger does not disclose the features recited in claim 62. To briefly summarize the pertinent features, claim 62 recites separating services from the service provider into two groups of services provided by two respective groups of one or more servers where the different groups of one or more servers have different trust relationships with the client computers – and those trusts are backwards with respect to each other. More specifically, claim 62 recites that there is a one-way trust connection *from* the first set of servers *to* the client computers and another one-way trust connection *from* the client computers *to* the second set of servers. Erpeldinger does not disclose these features.

The passage of Erpeldinger most pertinent to the above found by Applicants recites "a user may connect to several servers to use different services." See col. 1, lines 32-33. However, the quoted passage merely indicates that a user may access different services on different servers, but is completely silent, as is the rest of Erpeldinger, regarding the existence of differently directed one-way trust connections between the various sets of servers and the computers receiving services from the sets of servers. Accordingly, claim 62, and claims 64 and 65 which depend thereon, are patentable over Erpeldinger under 35 U.S.C. § 102 (e).

**C. The rejection of Claim 66 as Being Anticipated by Erpeldinger is Improper:**

Claim 66 is directed to a method for providing services from a service provider to a plurality of client computers and recites:

> enabling a first set of services on a first set of servers of the service provider through a one-way trust connection from the first set of servers to the plurality of client computers;
>
> enabling a second set of services on a second set of servers of the service provider to the plurality of client computers through a one-way trust connection from the client computers to the second set of servers; and
>
> providing the first and second sets of services.

As discussed to some extent in connection with claim 62 above, Erpeldinger does not disclose providing a first set of services through a one-way trust connection extending from a first set of servers to a plurality of client computers and a second set of services through another one-way trust connection extending from the client computers to a second set of servers. Accordingly, claim 66 is patentable over Erpeldinger under 35 U.S.C. § 102 (e).

**D. The rejection of Claim 67 as Being Anticipated by Erpeldinger is Improper:**

Claim 67 is directed to a system for providing services to a plurality of client computers and recites:

> a first set of servers for providing a first set of services to the plurality of client computers through a one-way trust relationship from the first set of servers to the plurality of client computers; and
>
> a second set of servers for providing a second set of services to the plurality of client computers through a one-way trust relationship from the plurality of client computers to the second set of servers.

Erpeldinger does not disclose providing a first set of services to a plurality of client computers through a one-way trust relationship extending from a first set of servers to the plurality of client computers and a second set of servers for providing a second set of services to the client computers using a one-way trust relationship extending from the client computers to the second set of servers. Accordingly, claim 67 is patentable over Erpeldinger under 35 U.S.C. § 102 (e).

**CONCLUSION**

For all of the reasons set forth above, the rejection of claims 40-44, 47-55, 58-62, and 64-67 as anticipated by Erpeldinger (U.S. Patent No. 6,557,169) should be reversed.

The Commissioner is hereby authorized to charge any further fees believed due from, or credit any overpayment to, our Deposit Account No.50-4711.

Dated: February 12, 2009

Respectfully submitted,

By: s/Leslie S. Garmaise/
Leslie S. Garmaise
Registration No.: 47,587

and

s/Jeffrey I. Kaplan/
Jeffrey I. Kaplan
Registration No.: 34,356

KAPLAN GILMAN & PERGAMENT LLP
1480 Route 9 North, Suite 204
Woodbridge, New Jersey 07095
732-636-4500
*Attorneys for Applicant*

F:\Clients\CenterBeam, Inc-300\300-2\300-2 Appeal Materials for OA of 9-23-08\300-2 Appeal Brief_FINAL.doc

## CLAIMS APPENDIX

40. A method for a service provider to provide services to a plurality of client computers, the method comprising:

providing a first set of services on a first set of one or more servers of the service provider to the plurality of client computers by providing secure access to the first set of one or more servers by the plurality of client computers, but prohibiting secure access to the plurality of client computers by the first set of one or more servers; and

providing a second set of services on a second set of one or more servers of the service provider to the plurality of client computers by providing secure access to the plurality of client computers by the second set of one or more servers, but prohibiting secure access to the second set of one or more servers by the plurality of client computers.

41. The method of claim 40 wherein said first set of services comprise data services.

42. The method of claim 41 wherein said second set of services comprise management and configuration services.

43. The method of claim 41 wherein said first set of services comprises at least one service selected from the group consisting of: virus protection services, remote access, backup, software sharing, and telephony services.

44. The method of claim 42 wherein said second set of services comprises at least one service selected from the group consisting of: security, password management, software updates, software distribution, and access control.

47. The method of claim 42 further comprising:

providing secure access to the first set of one or more servers by the second set of one or more servers.

48. The method of claim 42 further comprising:

preventing said first set of one or more servers from securely accessing resources in said second set of one or more servers.

49. The method of claim 42 wherein said first set of one or more servers providing said data services and said second set of one or more servers providing said management and configuration services are separate.

50. The method of claim 40 further comprising:

connecting said first set of one or more servers to at least one of the group consisting of: the Internet, a public switched telephone network, and a data network.

51. A system for providing services to a plurality of client computers, the system comprising:

a first set of one or more servers for providing a first set of services to the plurality of client computers by providing secure access to the first set of one or more servers by the plurality of client computers, but prohibiting secure access to the plurality of client computers by the first set of one or more servers; and

a second set of one or more servers for providing a second set of services to the plurality of client computers by providing secure access to the plurality of client computers by the second set of one or more servers, but prohibiting secure access to the second set of one or more servers by the plurality of client computers.

52. The system of claim 51 wherein said first set of services comprise data services.

53. The system of claim 52 wherein said second set of services comprise management and configuration services.

54. The system of claim 52 wherein said first set of services comprises at least one service selected from the group consisting of: virus protection services, remote access, backup, software sharing, and telephony services.

55. The system of claim 53 wherein said second set of services comprises at least one service selected from the group consisting of: security, password management, software updates, software distribution, and access control.

58. The system of claim 53 wherein the system is operable to provide secure access to the first set of one or more servers by the second set of one or more servers.

59. The system of claim 53 wherein said system is operable to:

prevent said first set of one or more servers from securely accessing resources in said second set of one or more servers.

60. The system of claim 53 wherein said first set of one or more servers providing said data services and said second set of one or more servers providing said management and configuration services are separate.

61. The system of claim 51 wherein said first set of one or more servers is connected to at least one of the group consisting of: the Internet, a public switched telephone network, and a data network.

62. A method for a service provider to provide services to a plurality of client computers, the method comprising:

separating the services provided by the service provider into a first group of services provided by a first group of one or more servers of the service provider, and a second group of services provided by a second group of one or more servers of the service provider;

providing the first set of services from the first set of servers through a one-way trust connection from the first set of servers to the client computers; and

providing the second set of services from the second set of servers to the client computers through a one-way trust connection from the client computers to the second set of servers.

64. The method of claim 62 wherein said first set of services comprises at least one service selected from the group consisting of: virus protection services, remote access, backup, software sharing, and telephony services.

65. The method of claim 62 wherein said second set of services comprises at least one service selected from the group consisting of: security, password management, software updates, software distribution, and access control.

66. A method for providing services from a service provider to a plurality of client computers, the method comprising:

enabling a first set of services on a first set of servers of the service provider through a one-way trust connection from the first set of servers to the plurality of client computers;

enabling a second set of services on a second set of servers of the service provider to the plurality of client computers through a one-way trust connection from the client computers to the second set of servers; and

providing the first and second sets of services.

67. A system for providing services to a plurality of client computers, the system comprising:

a first set of servers for providing a first set of services to the plurality of client computers through a one-way trust relationship from the first set of servers to the plurality of client computers; and

a second set of servers for providing a second set of services to the plurality of client computers through a one-way trust relationship from the plurality of client computers to the second set of servers.

.

## EVIDENCE APPENDIX

None.

## RELATED PROCEEDINGS APPENDIX

None.